CLAIMS

What is claimed is:

1. A method for authenticating a user certificate received from a user requesting access to a secure web service, said user certificate including user certificate data, said method comprising:

retrieving revoked certificate data from a plurality of certificate issuers, wherein the revoked certificate data identifies one or more revoked certificates;

storing the revoked certificate data in a central location;

receiving a request from a user for access to the web service, said request including the user certificate;

comparing the user certificate data included in the user certificate to the revoked certificate data stored in the central location;

selectively authenticating the user as a function of the comparing; and

providing the user access to the requested web service when the user is authenticated.

2. The method of claim 1, wherein the user certificate data includes a unique identifier identifying a particular certificate issued to the user, and wherein authenticating the user includes determining whether the unique identifier included with the request corresponds to a unique identifier included in the revoked certificate data.

3. The method of claim 1, wherein the user certificate data includes an expiration date identifying a date after which the certificate issued to the user is invalid, and wherein authenticating the user includes determining whether the expiration date is prior to a current date or after the current date, and providing the authenticated user access to the requested web service when the expiration date is determined to be after to the current date.

4. The method of claim 1, wherein retrieving the revoked certificate data from a plurality of certificate issuers includes:

identifying an address from the user certificate data included with the request, said address identifying the location of revoked certificate data for a plurality of revoked certificates being maintained by at least one of the plurality of certificate issuers; and

retrieving the revoked certificate data from the location identified by the identified address.

5. The method of claim 4, wherein the identified address is a uniform resource locator corresponding to a web service storing revoked certificate data.

6. The method of claim 4 further including comparing user certificate data to the retrieved revoked certificate data stored in the central location to identify a new a list of addresses corresponding to a plurality of different revoked certificates

7. The method of claim 4, wherein identifying the address from the user certificate data included with the request includes identifying the location of a certificate revocation list, said certificate revocation list listing revoked certificate data for a plurality of revoked certificate data being maintained by at least one of the plurality of certificate issuers

8. The method of claim 1, wherein the retrieving includes retrieving revoked certificates previously stored in the central location.

9. A method for adding additional revoked certificate data from a plurality of certificate issuers to revoked certificate data stored in a central location, said stored revoked certificate data identifying one or more certificate issuers publishing revoked certificate data for a plurality of revoked certificates, , comprising:

retrieving the stored revoked certificate data from the central location;

determining an update time for each of the one or more certificate issuers from the retrieved revoked certificate data, said update times each specifying a time updated revoked certificate data is published by each of the one or more certificate issuer;

organizing the retrieved revoked certificate data in a sequence according to the determined update time for each of the one or more certificate issuers;

identifying an address of each of the one or more certificate issuers from the retrieved revoked certificate data ; and

retrieving additional revoked certificate data from the identified addresses according to update times in the organized sequence.

10. The method of claim 9, wherein determining the update time includes parsing the retrieved revoked certificate data to determine update times, and wherein the identifying an address of a certificate issuer includes parsing the revoked certificate data to identify a uniform resource locator (URL) identifying an Internet address of the certificate issuer.

11. A system for retrieving revoked certificate data in response to a client request, said client request requesting access to a secure web service and including user certificate data, comprising:

a central database;

a fetching server for retrieving revoked certificate data from a plurality of certificate authority servers for storage in said central database, wherein the revoked certificate data identifies one or more revoked certificates; and

an authentication server responsive to the client request for executing a certificate revocation provider component, said certificate revocation provider component loading the revoked certificate data in the central database into a memory associated with the authentication server, and wherein the certificate revocation provider component is responsive to the client request and loaded revoked certificate data to determine if the client request is authentic.

12. The system of claim 11, wherein the certificate revocation provider service examines an expiration date included in the revoked certificate data to determine if the client is authorized to access the requested web service.

13. The system of claim 11, wherein the certificate revocation provider service further examines a next update time included in loaded revoked certificate data to determine if the loaded revoked certificate data is the latest revoked certificate data.

14. The system of claim 11, wherein the fetching server includes a default address identifying the location of a certificate authority server publishing revoked certificate data for a list of revoked certificates, and wherein the fetching server retrieves the revoked certificate data from the certificate authority having the default address.

15. The system of claim 11, wherein the fetching server includes a fetching table maintaining revoked certificate data for a plurality of revoked certificates previously retrieved from a certificate authority server, and wherein revoked certificate data maintained in the fetching table identifies an address of a certificate authority server maintaining a list of revoked certificates, and wherein the fetching server retrieves additional revoked certificate data from the certificate authority having the identified address.

16. The system of claim 15, wherein the certificate revocation provider service further compares retrieved revoked certificate data to user certificate data to identify a new a list of addresses corresponding to a plurality of revoked certificates.

17. A system for managing certificate revocation status data, comprising:

a fetching server for identifying a list of addresses corresponding to a plurality of certificate issuers, said fetching server retrieving revoked certificate status data from a content server corresponding to the list of addresses; and

a central database responsive to the retrieved revoked certificate status data for storing a list of revoked certificates.

18. A computer-readable medium comprising computer-executable instructions for authenticating a user requesting access to a web service, comprising

retrieving instructions for retrieving revoked certificate data from a plurality of certificate issuers, wherein the revoked certificate data identifies one or more revoked certificates;

storing instructions for storing the revoked certificate data for each of the identified one or more revoked certificates in a central location;

receiving instructions for receiving a request from a user for access to the web service, said request including a user certificate including user certificate data;

comparing instructions for comparing the user certificate data to the revoked certificate data stored in the central location; authenticating instructions for selectively authenticating the user as a function of the comparison; and

providing instructions for providing the user access to the requested web service when the user is authenticated.

19. The computer readable medium of claim 18 wherein user certificate data includes a unique identifier identifying a particular certificate issued to the user, and wherein authenticating the user includes instructions for determining whether the unique identifier included with the request corresponds to a unique identifier included in the revoked certificate data.

20. The computer readable medium of claim 18 wherein user certificate data includes an expiration date identifying a date after which the certificate issued to the user is invalid, and wherein authenticating the user includes instructions for determining whether the expiration date is prior to a current date or after the current date, and wherein providing instructions provide the identified authentic user access to the requested web service when the expiration date is determined to be after to the current date.

21. The computer readable medium of claim 18, wherein the instructions for retrieving the revoked certificate data from a plurality of certificate issuers include instructions for identifying an address from the user certificate data included with the request, said address identifying a location for revoked certificate data being published by at least one of the plurality of certificate issuers, and wherein the retrieving instructions include instructions for retrieving the revoked certificate data from the identified location.

22. A computer readable medium for adding additional revoked certificate data to revoked certificate data stored in a central location, said stored revoked certificate data identifying one or more certificate issuers publishing revoked certificate data for a plurality of revoked certificates, comprising:

retrieving instructions for retrieving the stored revoked certificate data from the central location;

determining instructions for determining an update time for each of the one or more certificate issuers from the retrieved revoked certificate data, said update times each specifying a time updated revoked certificate data is published by each of the one or more certificate issuer;

organizing instructions for organizing the retrieved revoked certificate data in a sequence according to the determined update time for each of the plurality of certificate issuers;

identifying instructions for identifying an address of each of the one or more certificate issuers from the organized revoked certificate data; and

retrieving instructions for retrieving additional revoked certificate data from the identified addresses according to update times in the organized sequence.